LISTING OF THE CLAIMS

CLAIMS

What is claimed, is:

1. (Currently amended) A method comprising ~~of~~ monitoring network activities as a time-ordered sequence of events in a computer network, each event having attributes triggered by an intrusion-detection system, each event being characterized by a given set of attributes called dimensions, each event forming an n-dimensional space, the step of monitoring ~~method~~ comprising:

said computer network triggering said events, each event being provided with attribute values allocated to a given set of attributes of said each event, each attribute having a particular attribute value,

simultaneously monitoring each particular attribute value of various event attributes from said given set of attributes versus the arrival time of said each event,

providing an event display with a cross plot having x and y coordinate axes, the x-axis presenting a time period and the y-axis presenting an attribute value range, and visualizing data along said x and y coordinate axes, said axes being attribute axes,

determining a primary attribute of said each event, said primary attribute being selected from the given set of attributes, each said primary attribute of said each event to be presented with ~~its~~ a corresponding attribute ~~values~~ value on the y-axis of the cross plot,

allocating a first display label to the events indicating the attribute ~~values~~ value of the primary attribute of each event, providing a pattern algorithm to detect whether an arrived event is part of the given pattern on the basis of a comparison of the attributes allocated to the given pattern and

of the attributes assigned to the arrived event, providing a mapping algorithm to map any attribute value of an attribute selected from the given set of attributes onto the y-axis of the cross plot,

allocating a second display label to said each event indicating the attribute values of the attributes being uncovered as part of the given pattern,

plotting all events that arrived within the time period and including an attribute value allocated to the primary attribute into the cross plot with the first display label indicating the primary attribute, the position of the first display label of said each event in the cross plot being determined on the basis of the attribute value of the primary attribute of the event and its arrival time,

plotting all events that arrived within the time period and being detected by means of the pattern algorithm as part of the given pattern into the cross plot with the second display label indicating the given pattern, the position of the second display label of said each event in the cross plot being determined by the mapping algorithm on the basis of the attribute value of the attribute of the event being uncovered as part of the given pattern and its arrival time,

viewing a secondary attribute of said each event together with the primary attribute on said display~~; and~~

~~automatically generating a large variety of visualizations along other attribute axes, and identifying correlations by superimposing and cross-referencing these visualizations~~.

2. (original) The method according to claim 1, further comprising:

recording the attribute values and the arrival time of a new event, determining on the basis of the recorded attribute values of event whether or not the newly arrived event includes an attribute value of the primary attribute, and if the newly arrived event includes the attribute value for the primary attribute shifting the x-axis of the cross plot so that the time period being presented on the x-axis covers the arrival time of the event, and

plotting the event arrived within the shifted time period into the cross plot with the first display label indicating the primary attribute.

3. (original) The method according to claim 2 comprising the further steps of:

determining on the basis of the recorded attribute values of event whether or not the newly arrived event is part of the given pattern on the basis of a comparison of the attributes allocated to the given pattern and of the attributes assigned to the arrived event,

if the newly arrived event includes an attribute value of the given pattern adding the event to the previous events being detected as part of the given pattern, and

redrawing all the events being associated with given pattern in the cross plot.

4. (previously presented) The method according to claim 3, further comprising:

if the newly arrived event does not include an attribute value of the given pattern, determining on the basis of the recorded attribute values of all previous arrived events by means of the pattern algorithm whether or not the newly arrived event is part of a new pattern on the basis of a comparison of the attributes allocated to the new pattern and of the attributes assigned to the arrived events;

if the newly arrived event forms together with previous recorded events the new pattern, allocating a third display label to the events indicating the attribute values of the attributes being uncovered as part of the new pattern; and

plotting the all events being detected by means of the pattern algorithm as part of the new pattern into the cross plot with the third display label indicating the new pattern, the position of the third display label of said each event in the cross plot being determined by the mapping algorithm on

the basis of the attribute value of the attribute of the event being uncovered as part of the new pattern and its arrival time.

5. (previously presented) The method according to claim 1 , further comprising:

removing all the events including an attribute value allocated to the primary attribute from the cross plot, if a primary attribute to be presented with its attribute values on the y-axis of the cross plot is changed, allocating a fourth display label to the events indicating the attribute values of the new primary attribute, and

plotting all the events arrived within the time period and including an attribute value allocated to the new primary attribute into the cross plot with the fourth display label indicating the new primary attribute, the position of the fourth display label of said each event in the cross plot being determined on the basis of the attribute value of the primary attribute of the event and its arrival time.

6. (original) The method according to claim 1 comprising the further steps of plotting all attribute values recorded for an event with the respective display label into the cross plot if the event is selected by an operator, and displaying textual information associated with the selected event on the event display.

7. (original) The method according to claim 1, wherein the pattern algorithm is suitable to perform multi-attribute pattern recognition.

8. (original) The method according to claim 1, wherein each display label includes a specific color and/or a specific mark layout.

9. (original) The method according to claim 1, wherein all events being uncovered as part of the pattern are clustered by the corresponding display label.

10. (Currently amended) A method according to claim 1, further comprising employing a computer readable program on tangible computer ~~media~~ readable medium and being computer executable instructions, comprising program code to cause the carrying out the steps of triggering, monitoring, providing, determining, allocating a first display label, allocating a second display label, plotting events including an attribute value, plotting events detected, viewing, and automatically generating, when the program code is running on a computer.

11. (Currently amended) A computer program *on a computer readable medium* ~~containing a~~ comprising program code being computer executable instructions to carry out all steps of the method of claim 1, said program code being stored on data carrier.

12. (previously presented) An event visualization device for monitoring events in a computer network, the device comprising means to perform all steps of the method as claimed in claim 1.

13. (previously presented) An article of manufacture comprising a computer readable medium having computer readable program code means embodied therein for causing monitoring of events in a computer network, the computer readable program code means in said article of manufacture comprising computer readable program code means for causing a computer to effect all steps of claim 1.

14. (Currently amended) A program storage device being a computer readable medium, tangibly embodying a program of instructions executable by ~~the machine~~ a computer to perform method steps for monitoring network activities as a time-ordered sequence of events in a computer network, each event having attributes triggered by an intrusion-detection system, each event being characterized by a given set of attributes called dimensions, each event forming an n-dimensional space, said step of monitoring ~~method steps~~ comprising the steps of:

said computer network triggering said events, each event being provided with attribute values allocated to a given set of attributes of said each event, each attribute having a particular attribute value,

simultaneously monitoring each particular attribute value of various event attributes from said given set of attributes versus the arrival time of said each event,

providing an event display with a cross plot having x and y coordinate axes, the x-axis presenting a time period and the y-axis presenting an attribute value range, and visualizing data along said x and y coordinate axes, said axes being attribute axes,

determining a primary attribute of said each event selected from the given set of attributes, each said primary attribute of said each event to be presented with ~~its~~ a corresponding attribute ~~values~~ value on the y-axis of the cross plot,

allocating a first display label to the events indicating the attribute ~~values~~ value of the primary attribute of each event providing a pattern algorithm to detect whether an arrived event is part of the given pattern on the basis of a comparison of the attributes allocated to the given pattern and of the attributes assigned to the arrived event, providing a mapping algorithm to map any attribute value of an attribute selected from the given set of attributes onto the y-axis of the cross plot,

allocating a second display label to said each event indicating the attribute values of the attributes being uncovered as part of the given pattern,

plotting all events that arrived within the time period and including an attribute value allocated to the primary attribute into the cross plot with the first display label indicating the primary attribute, the position of the first display label of said each event in the cross plot being determined on the basis of the attribute value of the primary attribute of the event and its arrival time,

plotting all events that arrived within the time period and being detected by means of the pattern algorithm as part of the given pattern into the cross plot with the second display label indicating the given pattern, the position of the second display label of said each event in the cross plot being determined by the mapping algorithm on the basis of the attribute value of the attribute of the event being uncovered as part of the given pattern and its arrival time, and

viewing a secondary attribute of said each event together with the primary attribute on said display~~; and~~

~~automatically generating a large variety of visualizations along other attribute axes, and identifying correlations by superimposing and cross-referencing these visualizations~~.

15. (previously presented) A computer program product comprising a computer readable medium having computer readable program code means embodied therein for causing the event visualization device, the computer readable program code means in said computer program product comprising computer readable program code means for causing a computer to effect all functions of claim 12.

16. (previously presented) The method according to claim 1, further comprising:

recording the attribute values and the arrival time of a new event, determining on the basis of the recorded attribute values of event whether or not the newly arrived event includes an attribute value of the primary attribute, and if the newly arrived event includes the attribute value for the primary attribute shifting the x-axis of the cross plot so that the time period being presented on the x-axis covers the arrival time of the event,

plotting the event arrived within the shifted time period into the cross plot with the first display label indicating the primary attribute;

determining on the basis of the recorded attribute values of event whether or not the newly arrived event is part of the given pattern on the basis of a comparison of the attributes allocated to the given pattern and of the attributes assigned to the arrived event;

if the newly arrived event includes an attribute value of the given pattern adding the event to the previous events being detected as part of the given pattern;

redrawing all the events being associated with given pattern in the cross plot;

if the newly arrived event does not include an attribute value of the given pattern, determining on the basis of the recorded attribute values of all previous arrived events by means of the pattern algorithm whether or not the newly arrived event is part of a new pattern on the basis of a comparison of the attributes allocated to the new pattern and of the attributes assigned to the arrived events;

if the newly arrived event forms together with previous recorded events the new pattern, allocating a third display label to the events indicating the attribute values of the attributes being uncovered as part of the new pattern; and

plotting the all events being detected by means of the pattern algorithm as part of the new pattern into the cross plot with the third display label indicating the new pattern, the position of the third display label of each event in the cross plot being determined by the mapping algorithm on the basis of the attribute value of the attribute of the event being uncovered as part of the new pattern and its arrival time;

17. (previously presented) The method according to claim 16, further comprising:

removing all the events including an attribute value allocated to the primary attribute from the cross plot, if a primary attribute to be presented with its attribute values on the y-axis of the cross

plot is changed, allocating a fourth display label to the events indicating the attribute values of the new primary attribute, and

plotting all the events arrived within the time period and including an attribute value allocated to the new primary attribute into the cross plot with the fourth display label indicating the new primary attribute, the position of the fourth display label of each event in the cross plot being determined on the basis of the attribute value of the primary attribute of the event and its arrival time.

18. (previously presented) The event visualization device for monitoring events in a computer network, according to claim 12, further comprising:

means for recording the attribute values and the arrival time of a new event, means for determining on the basis of the recorded attribute values of event whether or not the newly arrived event includes an attribute value of the primary attribute, and if the newly arrived event includes the attribute value for the primary attribute shifting the x-axis of the cross plot so that the time period being presented on the x-axis covers the arrival time of the event,

means for plotting the event arrived within the shifted time period into the cross plot with the first display label indicating the primary attribute;

means for determining on the basis of the recorded attribute values of event whether or not the newly arrived event is part of the given pattern on the basis of a comparison of the attributes allocated to the given pattern and of the attributes assigned to the arrived event;

means for adding for if the newly arrived event includes an attribute value of the given pattern adding the event to the previous events being detected as part of the given pattern;

means for redrawing all the events being associated with given pattern in the cross plot;

means for determining if the newly arrived event does not include an attribute value of the given pattern, means for determining on the basis of the recorded attribute values of all previous arrived events by means of the pattern algorithm whether or not the newly arrived event is part of a new pattern on the basis of a comparison of the attributes allocated to the new pattern and of the attributes assigned to the arrived events;

means for allocating if the newly arrived event forms together with previous recorded events the new pattern, allocating a third display label to the events indicating the attribute values of the attributes being uncovered as part of the new pattern; and

means for plotting the all events being detected by means of the pattern algorithm as part of the new pattern into the cross plot with the third display label indicating the new pattern, the position of the third display label of each event in the cross plot being determined by the mapping algorithm on the basis of the attribute value of the attribute of the event being uncovered as part of the new pattern and its arrival time;

19. (previously presented) The event visualization device for monitoring events in a computer network, according to claim 18, further comprising:

means for removing all the events including an attribute value allocated to the primary attribute from the cross plot, if a primary attribute to be presented with its attribute values on the y-axis of the cross plot is changed, allocating a fourth display label to the events indicating the attribute values of the new primary attribute, and

means for plotting all the events arrived within the time period and including an attribute value allocated to the new primary attribute into the cross plot with the fourth display label indicating the new primary attribute, the position of the fourth display label of each event in the cross plot being determined on the basis of the attribute value of the primary attribute of the event and its arrival time.

20. (currently amended) An article of manufacture comprising apparatus for monitoring events in a computer network, the apparatus comprising:

said computer network having means for intrusion-detection triggering said events, each event having attributes triggered by the means for intrusion-detection, each event being characterized by a given set of attributes called dimensions, each event forming an n-dimensional space, each event being provided with attribute values allocated to a given set of attributes of said each event,

means for simultaneously monitoring various event attributes from said given set of attributes versus the arrival time of said each event,

means for providing an event display with a cross plot having x and y coordinate axes, the x-axis presenting a time period and the y-axis presenting an attribute value range, and visualizing data along said x and y coordinate axes, said axes being attribute axes,

means for determining a primary attribute of said each event, said primary attribute being selected from the given set of attributes, each said primary attribute of said each event to be presented with ~~its~~ a corresponding attribute ~~values~~ value on the y-axis of the cross plot,

means for allocating a first display label to the events indicating the attribute ~~values~~ value of the primary attribute of each event, providing a pattern algorithm to detect whether an arrived event is part of the given pattern on the basis of a comparison of the attributes allocated to the given pattern and of the attributes assigned to the arrived event, providing a mapping algorithm to map any attribute value of an attribute selected from the given set of attributes onto the y-axis of the cross plot,

means for allocating a second display label to said each event indicating the attribute values of the attributes being uncovered as part of the given pattern,

means for plotting all events that arrived within the time period and including an attribute value allocated to the primary attribute into the cross plot with the first display label indicating the primary attribute, the position of the first display label of said each event in the cross plot being determined on the basis of the attribute value of the primary attribute of the event and its arrival time,

means for plotting all events that arrived within the time period and being detected by means of the pattern algorithm as part of the given pattern into the cross plot with the second display label indicating the given pattern, the position of the second display label of said each event in the cross plot being determined by the mapping algorithm on the basis of the attribute value of the attribute of the event being uncovered as part of the given pattern and its arrival time, and

means for viewing a secondary attribute of said each event together with the primary attribute on said display~~; and~~

~~means for automatically generating a large variety of visualizations along other attribute axes, and identifying correlations by superimposing and cross-referencing these visualizations~~.